

REMARKS

Applicant respectfully requests that the above-identified patent application be reexamined and reconsidered.

Claims 1-21 are now pending in this application. In an Office Action dated March 30, 2004 (hereinafter the "Office Action"), Claims 1-5, 8-13, 17, 19 and 21 were rejected under 35 U.S.C. § 103(a) as being unpatentable over U.S. Patent No. 6,263,432 to Sasmazel et al. (hereinafter "Sasmazel"), in view of U.S. Patent No. 5,721,777 to Blaze et al. (hereinafter "Blaze"), in view of U.S. Patent No. 6,101,486 to Roberts et al. (hereinafter "Roberts"), in further view of U.S. Patent No. 5,999,711 to Misra et al. (hereinafter "Misra"). Claims 6-7 were rejected under 35 U.S.C. § 103(a) as being unpatentable over Sasmazel in view of Blaze, Roberts, and Misra, and in further view of U.S. Patent No. 6,005,853 to Wang et al. (hereinafter "Wang"). Claims 14-16, 18, and 20 were rejected under 35 U.S.C. § 103(a) as being unpatentable over Sasmazel in view of Roberts, Blaze, and Misra, and in further view of U.S. Patent No. 5,481,539 to Hershey et al. (hereinafter "Hershey"). While applicant strongly believes that the previously presented claims were clearly allowable in view of the cited and applied references, in order to advance the prosecution of this application, a variety of language changes and clarifications have been made in order to make the claim language more particularly point out and distinctly claim the subject matter that applicant regards as the invention. Further, the incorrect dependency of Claim 10 has been corrected. (Prior to this amendment, Claims 9 and 10, which contain the same language, were both dependent from Claim 1.) Pursuant to 37 C.F.R. § 1.111 and for the reasons set forth below, applicant respectfully requests reconsideration and allowance of this application.

Prior to discussing in detail why applicant believes that all of the claims in the application are allowable, a brief description of applicant's invention and the cited references are provided.

LAW OFFICES OF
CHRISTENSEN O'CONNOR JOHNSON KINDNESS^{LLC}
1420 Fifth Avenue
Suite 2800
Seattle, Washington 98101
206.682.8100

-6-

MSPT\15431AM.DOC
06/30/04 4:59 PM

The following discussions of the disclosed embodiments of applicant's invention and the teachings of the applied references are not provided to define the scope or interpretation of any of applicant's claims. Instead, such discussed differences are provided to help the U.S. Patent and Trademark Office (hereinafter "the Office") better appreciate important claim distinctions discussed thereafter.

Summary of the Present Invention

The present invention allows users of a client computer to access a second server-based application based on previously provided authorization to access a first server-based application. The access to the second server-based application is based on previously provided access to a first server-based application that can securely authenticate a client computer without requiring a user to endure a lengthy log-in procedure.

The invention is ideally suited for use with client computers capable of concurrently executing multiple client application programs, such as an instant messaging client application and a Web browser application. The client computer may make requests to server-based applications. If the client computer is authorized to access a first server-based application, an authorization ticket will be transmitted to the client computer. The authorization ticket is encrypted and includes a time stamp indicating the time at which the authentication ticket was created. Once the client computer has been provided authorization to access the first server-based application, a client application starts an elapsed time counter.

In one implementation of the present invention, when a request is made by the client computer to access a second server-based application, the client application communicating with the first server-based application determines the session length based upon the elapsed time counter. The client application then concatenates the original authorization ticket, the session length, and a secret shared with the second server-based application. A hash function is then

LAW OFFICES OF
CHRISTENSEN O'CONNOR JOHNSON KINDNESS^{LLC}
1420 Fifth Avenue
Suite 2800
Seattle, Washington 98101
206.682.8100

applied to the concatenated data to create a unique hash value. The client stores the authorization ticket, the session length, and the hash value in a file that is accessible to a second client application executing on the client computer. The client also starts a persistence timer when the file is saved. The persistence timer is periodically checked to determine if a predetermined amount of time has lapsed. If the predetermined amount of time has elapsed, the file is deleted from the client computer.

The client application then launches the second client application and causes a log-in request to be transmitted from the second client application to the second server-based application. The request includes the file containing the authorization ticket, the session length, and the hash. The second client application then receives and displays results received from the second server-based application. When the second server-based application receives the log-in request, the authorization ticket is decrypted and the shared secret is obtained from a database. The second server-based application then compares the computed hash to the hash value received from the second client application. If the two hash values are identical, the second server-based application authorizes the client computer. As a result, a user does not experience multiple log-in procedures when accessing multiple server-based applications that service different client-based applications.

Summary of Sasmazel

Sasmazel purportedly discloses a system for authentication of data communications over a network that maintains user authorization throughout a network session. More specifically, Sasmazel purportedly allows a distributed system to maintain user authorization regardless of which computer in the distributed system handles the user request. Two server computers are used to authenticate a user and maintain that authentication throughout a network session—for example, a Web site visit. The first server is the "authentication server," which performs actions

LAW OFFICES OF
CHRISTENSEN O'CONNOR JOHNSON KINDNESS^{LLP}
1420 Fifth Avenue
Suite 2800
Seattle, Washington 98101
206.682.8100

necessary to authenticate a user. The second server is the function based "authorization server" that checks a user's authorization level. According to Sasmazel, the authentication server is the core of the system, serving to coordinate processes including receiving authentication information from a user and generating an eticket. The authorization server uses the information in the eticket to check authorization functionality.

Summary of Blaze

Blaze purportedly discloses a system for cryptographic key management that includes a smartcard that stores information about predetermined conditions under which an escrow agent is able to decrypt data files. Also, the Blaze system includes a tracking mechanism that records every time the smartcard is used for decryption. More specifically, Blaze purportedly discloses a portable cryptographic module (i.e., smartcard) that is configured to store programmed instructions whose execution grants access to cleartext data files. The programmed instructions may impose limitations on either the scope of information that is accessible to an escrow agent or limitations on when data files can be retrieved in cleartext form.

Summary of Roberts

Roberts purportedly discloses a system for automatically collecting profile information when a customer accesses a company Web site. After the profile information is known, dynamic content is displayed to the customer based on the customer's profile, which includes customized Web pages. The Roberts system for gathering customer profile data includes receiving user identification data and creating a customer profile. The customer profile is retrieved from a profile database when a call from the customer is received. Thereafter, the customer profile is compared to marketing material maintained by the company and a dynamic content message is generated for display on the customer computer.

LAW OFFICES OF
CHRISTENSEN O'CONNOR JOHNSON KINDNESSSM
1420 Fifth Avenue
Suite 2800
Seattle, Washington 98101
206.682.8100

Summary of Misra

Misra is purportedly directed to a system that has a facility to check authorization and authentication information in a distributed environment. The system includes a principal, such as a portable computer that holds a secure package for the principal. The secure package may be encrypted or may include a digital signature. Once the principal has been provided with the secure package, the principal may send a request to log in to the distributed system along with authorization and authentication information. The secure package is accessed to determine whether the principal is authorized to connect to the distributed system. Where the principal is not authorized to connect to the distributed system, the principal's request to log in is denied. In contrast, where the principal is authorized to connect to the distributed system, the principal's request to connect is granted.

Summary of Wang

Wang is purportedly directed to a channel access protocol for implementing a wireless data network. More specifically, Wang discloses a network protocol for a high channel utilization. The resulting network access scheme allows a transmitter to send messages to a cellular base station, simultaneously with other transmitters, without the need for retransmission, if the message reaches the receiver with sufficient strength. Multiple transmitters and receivers are distributed over a geographical area, sharing the same frequency channels. As a result, multiple messages are able to capture multiple receivers simultaneously, thereby improving the channel utilization. A message received by a base station is forwarded, either by a wired link or wireless link, to a network control center for routing. The base stations are distributed over a service area in accordance with the expected density of the wireless terminals and the physical attributes of the terrain.

LAW OFFICES OF
CHRISTENSEN O'CONNOR JOHNSON KINDNESS^{LLC}
1420 Fifth Avenue
Suite 2800
Seattle, Washington 98101
206.682.8100

Summary of Hershey

Hershey is purportedly directed to a system for communicating between mobile telephone devices. More specifically, Hershey purportedly discloses a communication protocol where a mobile unit creates a message packet that it desires to transmit to an intended receiver having a unique identification number, such as a mobile telephone number. The initiating mobile unit broadcasts the message packet in low power to local mobile units in the reception area. Each mobile unit that receives the message without errors responds with an acknowledgement signal. Each mobile unit that receives the broadcast determines if the message packet is valid. The mobile units compare the mobile unit identification number of valid message packets with its own internal identification number. If the identification numbers match, the message was successfully transmitted to the intended mobile unit.

I. Rejection of Claims 1-5, 8-13, 17, 19, and 21 Under 35 U.S.C. § 103

The Office Action rejected Claims 1-5, 8-13, 17, 19, and 21 under 35 U.S.C. § 103(a) as being unpatentable over Sasmazel, in view of Blaze, Roberts, and in further view of Misra. The Office Action asserts that Sasmazel, Blaze, Roberts, and Misra suggest each and every element of Claims 1-5, 8-13, 17, 19, and 21, and that it would be obvious to combine their teachings. Applicants respectfully disagree.

A. Claim 1

Claim 1, as amended, recites:

1. A method for authorizing a client computer to access a second server-based application based upon previously provided authorization to access a first server-based application, comprising:
 - (a) receiving a request to access said second computer server-based application;
 - (b) in response to said request:

LAW OFFICES OF
CHRISTENSEN O'CONNOR JOHNSON KINDNESS^{LLC}
1420 Fifth Avenue
Suite 2800
Seattle, Washington 98101
206.682.8100

- (i) determining a session length indicating a length of time said client computer has been authorized to access said first server-based application;
- (ii) calculating a hash value for an authorization ticket received from said first server-based application, said session length, and a secret shared between said client computer and said second server-based application, and
- (iii) transmitting a request for authorization to said second server-based application comprising said hash value, said authorization ticket, and said session length.

As distinctly recited in Claim 1, applicant's invention includes a method for authorizing a client computer to access a first server-based application. Once the client computer is authorized to access the first server-based application, a request to access a second server-based application is also authorized. A user associated with the client computer does not have to endure a second log-in procedure when making a request to access the second server-based application.

Conversely, Sasmazel is directed to a system that maintains user authorization throughout a network session. With the explosive popularity of the Internet, there is a rapidly growing need to provide unprecedented access to Web content. This need has created a strong demand for scalable Web servers as most popular Web sites are experiencing overload from an increasing number of users concurrently accessing the sites. Thus Web servers should be capable of handling a large number of concurrent requests simultaneously, with reasonable response times and minimal drop rates. Sasmazel is directed to a system that allows a Web server to satisfy requests without requiring user authorization when requests are handled by different computers.

As known to those skilled in the art and others, Web servers are typically supported by multiple computers connected in a local network. In this type of system, the Web server is said to be distributed as user requests are satisfied by any one of a number of computers in the local network. Sasmazel supports distributed servers by allowing users to remain authorized regardless of the computer that satisfies the Web request. More specifically, Sasmazel states that

LAW OFFICES OF
CHRISTENSEN OCONNOR JOHNSON KINDNESS^{LLC}
1420 Fifth Avenue
Suite 2800
Seattle, Washington 98101
206.682.8100

it "will provide a much more confined user and World Wide Web based application system by providing a user session concept with the 'eticket' architecture. **This ticketing architecture will tie the user browser to the Internet Server (or application).**" (Emphasis added). Sasmazel at Col. 10, lines 40-45. The ticketing architecture disclosed in Sasmazel is purportedly an improvement over a ticketing architecture that ties authorization to a specific computer.

Sasmazel does not disclose a method for authorizing a client computer to access a second server-based application based upon previously provided authorization to access a first server-based application. Instead, Sasmazel discloses a system where an eticket is "passed from server to server, without the user having to 'reauthenticate' each time a new server accesses the information. That is, a user does not have to 're-authenticate' all of the authentication information each time a new server is accessed." Sasmazel at Col. 8, lines 46-50. Stated differently, Sasmazel purportedly discloses a system where authentication is not connected to a specific computer. Instead, authentication is tied to an application such as a Web server that is distributed among multiple computers. Conversely, the present invention authorizes users to access multiple server-based applications that may or may not be located on different computers. Thus, the present invention is not limited to authorizing a user to access a specific application.

Claim 1 of the present invention recites a method for authorizing a client computer to access a second server-based application based upon previously provided authorization to access a first server-based application. More specifically, the claimed method recites (a) calculating a hash value for an authorization ticket received from said first server-based application, and (b) transmitting a request for authorization to said second server-based application comprising said hash value, said authorization ticket, and said session length. There are several distinctions between the present invention as recited in Claim 1 and the system disclosed in Sasmazel. For example, as described previously, the Sasmazel authentication system is tied to an application,

LAW OFFICES OF
CHRISTENSEN O'CONNOR JOHNSON KINDNESS^{LLC}
1420 Fifth Avenue
Suite 2800
Seattle, Washington 98101
206.682.8100

such as a Web server application, that is distributed among multiple computers. However, Sasmazel does not disclose a system where a user may access a "second server-based application" based on the previously provided log-in information. For example, Sasmazel does not disclose a system where a user may access a chat server, email server, or any other "server-based application" with the previously provided log-in information. Conversely, as recited in Claim 1, the present invention authorizes users to access multiple "server-based applications." For example, a user who provided log-in information to a chat server may then access a Web server, an email server, or any other server-based application that the user is authorized to access. Thus, Sasmazel does not disclose a method for authorizing a client computer to access a second server-based application based upon previously provided authorization to access a first server-based application.

The Office Action admits that Sasmazel does not specifically disclose "determining a session length indicating a length of time" the user is authorized to access a server-based application. However, the Office Action asserts that Blaze discloses determining a session length indicating a length of time the user is authorized to access a server-based application and references Col. 2, lines 34-36, of Blaze in support of that proposition. Applicant respectfully disagrees.

Blaze purportedly discloses a system for cryptographic key management that includes a smartcard that stores information about conditions under which an escrow agent is allowed to decrypt data files. More specifically, Blaze purportedly discloses a portable cryptographic module (i.e., smartcard) that is configured to store programmed instructions whose execution grants access to cleartext data files. As stated in Blaze, the "smartcard uses a clock to start a time, ascertain the date and time at which the file decryption occurred, and store such time and date in appropriate fields." (Emphasis added.) Blaze at Col. 6, lines 59-61. Similar to the

LAW OFFICES OF
CHRISTENSEN O'CONNOR JOHNSON KINDNESS^{LLC}
1420 Fifth Avenue
Suite 2800
Seattle, Washington 98101
206.682.8100

present invention, Blaze determines the time that specified events occur. However, unlike the present invention, Blaze does not disclose determining a session length indicating a length of time the user is authorized to access a server-based application. Instead, Blaze stores data related to the use of a smartcard and allows access to this information in response to a query. Storing time and date information related to the use of a smartcard is not the same as determining a session length that indicates a length of time a user is authorized to access a server-based application.

For at least the above-mentioned reasons, applicant respectfully submits that the Office Action has not established a *prima facie* case for a Section 103(a) rejection of Claim 1, and respectfully requests that the rejection of Claim 1 and the claims dependent thereon be withdrawn and these claims allowed.

B. Claim 13

Claim 13, as amended, recites:

13. A method for authorizing a client computer to access a second server-based application based upon previously provided authorization to access a first server-based application, comprising:

- (a) receiving a request for authorization to access said second server-based application from said client computer comprising a hash value, an authorization ticket, and a session length;
- (b) computing a new hash value for said authorization ticket, said session length, and a copy of a secret shared between said client computer and said second server-based application;
- (c) determining whether said hash value received from said client computer is identical to said new hash value; and
- (d) in response to determining that said hash value received from said client computer is identical to said new hash value, authorizing said client computer to access said second server-based application.

Claim 13 of the present invention recites a method for authorizing a client computer to access a second server-based application based upon previously provided authorization to access

LAW OFFICES OF
CHRISTENSEN O'CONNOR JOHNSON KINDNESS^{LLC}
1420 Fifth Avenue
Suite 2800
Seattle, Washington 98101
206.682.8100

a first server-based application. More specifically, the claimed method recites (a) receiving a request for authorization to access said second server-based application from said client computer comprising a hash value, an authorization ticket, and a session length, (b) computing a new hash value for said authorization ticket, said session length and a copy of a secret shared between said client computer and said second server-based application, and (c) in response to determining that said hash value received from said client computer is identical to said new hash value, authorizing said client computer to access said second server-based application.

As described previously with regard to Claim 1, Sasmazel does not disclose a method for authorizing a client computer to access a second server-based application based upon previously provided authorization to access a first server-based application. Instead, Sasmazel purportedly discloses a system where authentication is tied to a single application, such as a Web server application, that is distributed among multiple computers. Conversely, the present invention authenticates users to access multiple server-based applications that may or may not be located on different computers. Thus, the present invention is not limited to authorizing a user to access a specific application. Consequently, Sasmazel does not disclose the elements as recited in Claim 13, and applicant respectfully submits that the rejection of Claim 13 is in error and requests that the rejection be withdrawn.

The Office Action admits that Sasmazel does not specifically disclose "including a session length in the request for authorization." However, the Office Action asserts that Roberts discloses including a session length in the request for authorization and references, Col. 5, lines 2-24, of Roberts in support of that proposition. Applicant respectfully disagrees.

Roberts purportedly discloses a system for automatically collecting customer profile information when a customer accesses a company Web site. After the customer profile information is known, dynamic content is selected and displayed in accordance with the profile

LAW OFFICES OF
CHRISTENSEN O'CONNOR JOHNSON KINDNESS^{LLC}
1420 Fifth Avenue
Suite 2800
Seattle, Washington 98101
206.682.8100

information. The Roberts system for gathering customer profile information includes logging a customer's passive activity (i.e., time spent viewing a particular Web page). The Office inferred that the time spent viewing a particular Web page is substantially similar to a session length. Office Action at page 7. However, logging a customer's passive activity is not the same as "including a session length in the request for authorization." In fact, Roberts does not involve authenticating users to access any Web content. Instead, Roberts is only concerned with monitoring customers and providing customized Web pages.

For at least the above-mentioned reasons, applicant respectfully submits that the Office Action has not established a *prima facie* case for a Section 103(a) rejection of Claim 13 and respectfully requests that the rejection of Claim 13 and the claims dependent thereon be withdrawn.

C. Claims 2-5, 8-12, 17, 19, and 21

Since Claims 2-5 and 8 depend, directly or indirectly, from Claim 1 and Claims 9-10 and 11-12 are computer apparatus and computer-readable medium claims that depend from Claims 1 and 2. Thus, the analysis applied to Claim 1 also applies to these claims. Also, since Claim 21 depends from Claim 13 and Claims 17 and 19 are computer-controlled apparatus and computer-readable medium claims that depend from Claim 13, the analysis applied to Claim 13 also applies to these claims. Therefore, applicant respectfully submits that Claims 2-5, 8-12, 17, 19, and 21 are in condition for allowance for the same reasons as Claims 1 and 13, respectively. In addition, applicant submits that the dependent claims are allowable for additional reasons described below.

Claim 2 recites a combination of steps "wherein said authorization ticket comprises a time stamp, and wherein determining a session length comprises subtracting said time stamp from an elapsed time counter to determine said session length." The Office Action states that

LAW OFFICES OF
CHRISTENSEN O'CONNOR JOHNSON KINDNESSSM
1420 Fifth Avenue
Suite 2800
Seattle, Washington 98101
206.682.8100

"Misra teaches that the authorization ticket comprises a time stamp," and takes Official Notice that computing a session length by subtracting a timestamp from an elapsed time counter is well known in the art. However, applicant is unable to find any reference in Misra to a time counter or any other mechanism for determining a session length. Applicant respectfully agrees that time stamps are generally known in the art. However, the claimed combination of determining a session length based on the value of an elapsed time counter is not well known in the art. Therefore, applicant respectfully submits that Claim 2 is also in condition for allowance for these additional reasons.

Dependent Claims 3-4 add to the nonobviousness of applicant's invention of starting the elapsed time counter "when said authorization ticket is received from said first server-based application." The Office Action states that "Blaze teaches that the elapsed time counter is started when said authorization ticket is received" Office Action at page 5. However, applicant submits that Blaze only stores data related to the use of a smartcard. Storing time and date information related to the use of a smartcard is not the same as determining when to start an elapsed time counter. Therefore, applicants respectfully submit that Claims 3 and 4 are also in condition for allowance for these additional reasons.

Dependent Claim 5 adds to the nonobviousness of applicants' invention of "performing an MD5 hash of an authorization ticket received from said first server-based application, said session length, and a secret shared between said client computer and said second server-based application." The Office Action asserts that Sasmazel teaches performing an MD5 hash of an authorization ticket that includes a session length and a shared secret, and references Col. 2, lines 41-42, of Sasmazel in support of that proposition. The referenced section of Sasmazel states that an MD5 protocol is used to "hash the information in the data packet." However, Sasmazel indicates that the data packet only includes "authorization information." Sasmazel at

LAW OFFICES OF
CHRISTENSEN O'CONNOR JOHNSON KINDNESS^{LLC}
1420 Fifth Avenue
Suite 2800
Seattle, Washington 98101
206.682.8100

Col. 2, lines 32-33. The present invention provides a more secure environment by hashing data in addition to authentication information. More specifically, Claim 5 recites "performing an MD5 hash of an authorization ticket that includes a session length and a secret." Obviously, a session length stored on a client computer is not the same as authentication information. Therefore, applicants respectfully submit that Claim 5 is also in condition for allowance for these additional reasons.

Dependent Claims 8 and 21 add to the nonobviousness of applicants' invention by specifying that the first server-based application is an instant messaging server and specifying that the second server-based application is a Web server. The Office Action asserts that Sasmazel teaches "that the first computer comprises an instant messaging server computer (i.e., Web server) and that the second computer comprises a Web server computer." Office Action at page 6. The Office Action equates an instant messaging server with a Web server. However, an instant messaging server is not equivalent to a Web server. As known to those skilled in the art and others, an instant messaging server is used to establish "chat" sessions between client computers connected to a network. Conversely, a Web server transmits files such as hypertext documents between a server computer and a client computer. Therefore, applicants respectfully submit that Claims 8 and 21 are also in condition for allowance for these additional reasons.

II. Rejection of Claims 6-7 Under 35 U.S.C. § 103

The Office Action rejected Claims 6-7 under 35 U.S.C. § 103(a) as being unpatentable over Sasmazel, in view of Blaze, Roberts, and Misra, as applied to Claim 1 and further in view of Wang. The Office Action asserts that Sasmazel, Blaze, Roberts, Misra, and Wang suggest each and every element of Claims 6-7 and that it would be obvious to combine their teachings. Applicant respectfully disagrees. Since Claims 6-7 depend from Claim 1, the analysis applied to

LAW OFFICES OF
CHRISTENSEN O'CONNOR JOHNSON KINDNESS^{LLC}
1420 Fifth Avenue
Suite 2800
Seattle, Washington 98101
206.682.8100

Claim 1 also applies to these claims. In addition, applicant submits that these dependent claims are allowable for additional reasons described below.

Dependent Claim 6 adds to the nonobviousness of applicant's invention the combination of (1) starting a persistence timer; (2) determining whether said persistence timer has reached a predefined value prior to receiving a response from said server-based application; and (3) in response to determining that said persistence timer has reached a predefined value prior to receiving a response from said second server-based application, deleting said authorization ticket, said session length and said hash value from said client computer." The Office Action asserts that Wang teaches these additional elements recited in Claim 6, stating that "Wang teaches that when a data packet (i.e., authentication ticket) is sent, a sequence variable is allocated and an acknowledgement timer (i.e., persistence timer) is set to prevent waiting indefinitely." Office Action at page 9. However, a system that prevents deadlocks (i.e., waiting indefinitely) as disclosed in Wang is not equivalent to the elements recited in Claim 6. More specifically, Claim 6 recites using a persistence timer to periodically check to determine if a predetermined amount of time has elapsed. This is not equivalent to using an acknowledgement timer to prevent deadlocks. Therefore, applicant respectfully submits that Claim 6 is also in condition for allowance for these additional reasons.

Dependent Claim 7 adds to the nonobviousness of applicant's invention the combination of "in response to determining that said persistence timer has not reached a predefined value prior to receiving a response from said second server-based application, receiving said response from said second server-based application and displaying said response at said client computer." The Office Action asserts that Wang teaches the additional elements recited in Claim 7. However, applicant is unable to find any reference in Wang to displaying the results of an authentication process. Instead, Wang is directed to a channel access protocol for implementing

LAW OFFICES OF
CHRISTENSEN O'CONNOR JOHNSON KINDNESS^{PLLC}
1420 Fifth Avenue
Suite 2800
Seattle, Washington 98101
206.682.8100

a wireless data network that does not involve interactions with a user. Therefore, applicant respectfully submits that Claim 7 is also in condition for allowance for these additional reasons.

III. Rejection of Claims 14-16, 18, and 20 Under 35 U.S.C. § 103

The Office Action rejected Claims 14-16, 18, and 20 under 35 U.S.C. § 103(a) as being unpatentable over Sasmazel, in view of Blaze, Roberts, and Misra as applied to Claim 13 and further in view of Hershey. The Office Action asserts that Sasmazel, Blaze, Roberts, Misra, and Hershey suggest each and every element of Claims 14-16, 18, and 20. Applicant respectfully disagrees.

A. Claims 14-16

Since Claims 14-16 depend from Claim 13, the analysis applied to Claim 13 also applies to these claims. In addition, applicant submits that these dependent claims are allowable for additional reasons described below.

Dependent Claims 14-16 add to the nonobviousness of applicant's invention the combination of "(1) in response to determining that said hash value received from said client computer is identical to said new hash value, (2) determining whether a sum of said session length and a time stamp received as part of said authorization ticket is within a preset threshold value of a current time, and (3) in response to determining that the sum of said session length and said time stamp is within said preset threshold value, authorizing said client computer to access said second server-based application." The Office Action asserts that Hershey teaches these additional elements and cites Col. 7, lines 34-43, of Hershey in support of that proposition. Applicant submits that Hershey does not authorize client computers to access any server-based application. Instead, the system disclosed in Hershey determines if "the current message packet has expired" using a time stamp. Hershey at Col. 7, lines 38-40. If the message packet has not expired, then the message is rebroadcast. Applicant submits that rebroadcasting a message

LAW OFFICES OF
CHRISTENSEN O'CONNOR JOHNSON KINDNESS^{PC}
1420 Fifth Avenue
Suite 2800
Seattle, Washington 98101
206.682.8100

packet based on a time stamp is not equivalent to "authorizing said client computer to access said second server-based application." Therefore, applicant respectfully submits that Claims 14-16 are also in condition for allowance for these additional reasons.

B. Claims 18 and 20

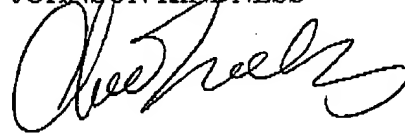
Since Claims 18 and 20 are directed to computer apparatus and computer-readable mediums having language that depend from Claim 14. Thus the analysis applied to Claim 14 also applies to these claims. Therefore, applicant respectfully submits that Claims 18 and 20 are in condition for allowance for the same reasons as Claim 14.

CONCLUSION

In view of the remarks above, applicant respectfully submits that the present application is in condition for allowance. Reconsideration and reexamination of the application and allowance of the claims at an early date are solicited. If the Examiner has any questions or comments concerning this matter, the Examiner is invited to contact the applicant's undersigned attorney at the number below.

Respectfully submitted,

CHRISTENSEN O'CONNOR
JOHNSON KINDNESS^{PLLC}

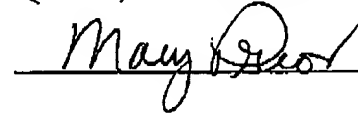


Clint J. Feekes
Registration No. 51,670
Direct Dial No. 206.695.1633

I hereby certify that this correspondence is being transmitted via facsimile to the U.S. Patent and Trademark Office, Group Art Unit 2131, Examiner Edel H. Quiñones, at facsimile number 1-703-872-9306 on June 30, 2004.

Date: June 30, 2004

CJF:mgp



LAW OFFICES OF
CHRISTENSEN O'CONNOR JOHNSON KINDNESS^{PLLC}
1420 Fifth Avenue
Suite 2800
Seattle, Washington 98101
206.682.8100